CEA ACTION PROPOSAL

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date: 2023-05-23

2. Department: Government Operations Agency

3. Organizational Placement (Division/Branch/Office Name)

4. CEA Position Title

Chief Privacy Officer

5. Summary of proposed position description and how it relates to the program's mission or purpose. (*2-3 sentences)*

The Chief Privacy Officer (CPO) will work collaboratively with GovOps' control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state.

6. Reports to: (*Class Title/Level*)

Deputy Secretary & Chief Counsel (Exempt)

7. Relationship with Department Director (*Select one)*

☑ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.

☐ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(*Explain*):

8. Organizational Level *(Select one)*

☐ 1st ☐ 2nd ☑ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

Under the general direction of the Chief Counsel, the Chief Privacy Officer (CPO) will work collaboratively with GovOps' control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state. The CPO will be responsible for policy and process analysis and development, vetting of technologies involving the collection of data, analysis of data sharing projects, advocacy, privacy assessment activities, and special projects. The CPO will lead the advancement and expansion of privacy-forward practices throughout state operations by building a culture of privacy, preserving public trust, and fostering innovation while safeguarding personal information.

Functions as the subject matter expert and principal policymaker for GovOps in the area of privacy law, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the California Information Practices Act (IPA), and other state and federal and statutory schemes. Evaluates privacy risk in GovOps reporting entities. Works with GovOps departments to establish appropriate policies and practices for the retention and disposal of data according to business use and risk. Develops appropriate response plans according to risk level. Evaluates contracts and practices of existing vendors that process or use State data to ensure compliance with privacy standards. In collaboration with the Chief Data Officer at ODI, assist in data inventory and classification activities. Develops and maintains appropriate communications, oversight, and training practices in preparation for privacy incidents. Consults with the Secretary, Undersecretary, and Executive staff and provides legal advice, significant policy creation, and program management on all matters concerning state and federal laws, regulations, policies, and procedures related to privacy. Acts as the lead in developing and overseeing privacy training, reviewing privacy legislation, and providing general privacy review for internal and external stakeholders.

Stays abreast of emerging issues at the local, state, and federal levels related to privacy. When appropriate, weighs in on pending federal or state legislation and recommends an effective course of action to the Secretary or Undersecretary. Brings together experts in academia, business, advocacy groups, and government to discuss privacy practices and develop and implement solutions that better protect people and organizations.

Works collaboratively with GovOps control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies, procedures, and business processes across the state.

Performs privacy impact assessments and information inventory on state operations. Examples include an assessment of all databases that store data within our control agency departments as well as collaborating with the GovOps reporting department's Chief Information Security Officers and the Chief Data Officer as needed. The CPO will respond to and track privacy-related incidents and data breaches.

Leads special projects and produces reports on an as-needed basis. Examples of this type of work include projects within ODI and/or CDT, the Statewide Data Strategy, monitoring and assessment approaches, data sharing coordination and reviews, and policy analysis and development.

Represent the Agency and/or Administration in meetings with legislators and staff, the State Controller's Office, the Department of Finance, other state departments, and interested stakeholders.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

- ☑ Program is directly related to department's primary mission and is critical to achieving the department's goals.
- ☐ Program is indirectly related to department's primary mission.
- ☐ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: The mission of the Government Operations Agency's (Agency) mission is to improve government operations within state departments so they can better serve the people of California. The Chief Privacy Officer will work collaboratively with GovOps' control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state. The CPO will lead policy and process analysis and development, vetting of technologies involving the collection of data, analysis of data sharing projects, advocacy, privacy assessment activities, and special projects. The CPO will advance and expand privacy-forward practices throughout state operations by building a culture of privacy, preserving public trust, and fostering innovation while safeguarding personal information.

The CPO will perform a privacy impact assessment and information inventory on state operations. Examples include an assessment of all databases that store data within GovOps control agency departments as well as collaborating with the GovOps reporting department's Chief Information Security Officers and the Chief Data Officer as needed. The CPO will help respond to and track privacy related incidents and data breaches.

The CPO will work collaboratively with GovOps control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

Privacy laws exist at the federal, state, and local levels. GovOps Information management practices and those of our reporting departments must be consistent with the Information Practices Act (Civil Code Section 1798 et seq.). This law applies to state government. It expands upon the constitutional guarantee of privacy by providing limits on the collection, management and dissemination of personal information by state agencies. The Public Records Act (Government Code Section 6250 et seq.), In enacting this chapter, the Legislature, mindful of the right of individuals to privacy, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. Government Code Sections 11015.5 and 11019.9, Each state department and state agency shall enact and maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Title 1.8 (commencing with Section 1798) of Part 4 of Division 3 of the Civil Code). Other applicable federal laws pertaining to information privacy. These statutes along with federal privacy requirements create a complex set of requirements which state departments must follow. GovOps through its oversight of the control agency departments is required to ensure that the appropriate privacy laws are implemented throughout state operations in order to avoid inappropriate disclosure of, or inappropriate collection of, information. The CPO will ensure that all laws are met and followed by GovOps and GovOps reporting departments.

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

As a member of GovOPS's executive team, the CEA is responsible for oversight of all operational needs and support necessary for privacy. The CEA will represent GovOPS's interests, recommending strategy, and providing project oversight by driving timelines, setting performance expectations and evaluating outcomes using metrics, and ensuring efficacy of products delivered for both internal and external stakeholders. The CEA's role in setting policy will include evaluating, advising, and providing assistance to the Undersecretary and Secretary on:

1. Work collaboratively with GovOps' control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state.

2. Will support policy and process analysis and development, vetting of technologies involving the collection of data, analysis of data sharing projects, advocacy, privacy assessment activities, and special projects.

3. Functions as the subject matter expert and policymaker for GovOps in the area of privacy law, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the California Information Practices Act (IPA), and other state and federal and statutory schemes.

Successful implementation and coordination of GovOPS initiatives have far reaching in impact, highly visible, and sometimes involving sensitive issues regarding sustainability efforts and emergency response activities. These issues have statewide impact on various stakeholder groups. Such responsibilities may elicit scrutiny from the Legislature, federal government, other state agencies, the media, and the public.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

Under the general direction of the Chief Counsel, the Chief Privacy Officer (CPO) will work collaboratively with GovOps' control agency departments to promote the privacy of the data they collect and use and ensure privacy is considered in all employee-related policies procedures, and business processes across the state. The CPO will support policy and process analysis and development, vetting of technologies involving the collection of data, analysis of data sharing projects, advocacy, privacy assessment activities, and special projects. The CPO will help to advance and expand privacy-forward practices throughout state operations by building a culture of privacy, preserving public trust, and fostering innovation while safeguarding personal information

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The CEA will both develop and implement new policy, as well as interpret and implement existing policy. The incumbent must possess an understanding of existing policies and business procedures that impact the Agency and all of the regulations that relate to privacy. They must also be aware of new laws that have been passed and that are being proposed by the California Legislature. As changes occur, the CEA will be responsible for developing and implementing new policy to ensure the Agency is in compliance with new legislation. They will work with the Agency's Executive Management Team, their peers, staff in other units, and their team members (staff and subordinate supervisors) to establish the best policies for the Agency. The incumbent must also be forward-looking, and be aware of what's on the horizon to ensure policies and procedures can be easily updated to accommodate evolving business and department needs. Internally, the CEA will be responsible for evaluating the needs of stakeholders and employees and developing or updating existing policy to ensure operational programs provide timely and accurate information to stakeholders.